PRBIT - Princípy bezpečnosti informačných technológií

Report - Domáca úloha č.2

Autor: Marek Čederle

Cvičenie: Pondelok 17:00

Použité príkazy a ich vysvetlenie

Zadanie č.1

- **Úlohy:**
  - vytvoriť šifrovaný (pomocou LUKS) súborový systém EXT4 v súbore s veľkosťou 32MiB,
  - nastaviť názov (label) na 'crypt_fs', počet pripojení pred testom nastaviť na 15, vyhradiť 3% kapacity pre root-a.
  - Pripojiť šifrovaný súborový systém
    - s podporou ACL a kvót, bez možnosti spúšťať programy,
    - mount point /tmp/crypt,
    - Vyskúšať spustenie programu z '/tmp/crypt'.

Najskôr som si vytvoril testovací priečinok `cviko2` a tam som pokračoval so zadaním.

```
mkdir ~/cviko2
cd ~/cviko2
dd if=/dev/zero of=fs.crypt bs=1M count=32
```

- `dd` - príkaz na konvertovanie a kopírovanie súborov
  - `if` - prepínač, ktorý určuje vstupný súbor
  - `/dev/zero` - špeciálny súbor, ktorý obsahuje nuly
  - `of` - prepínač, ktorý určuje výstupný súbor
  - `fs.crypt` - názov súboru, ktorý sa vytvorí
  - `bs` - prepínač, ktorý určuje veľkosť bloku (1M - 1 MiB)
  - `count` - prepínač, ktorý určuje počet blokov (32 - 32 MiB)

Nasledujúci príkaz vytvorí nové loop zariadenie `/dev/loop0` (pretože som na sytéme nemal okrem /dev/loop-control iné loop zariadenie).

```
sudo losetup -f
```

- `losetup` - príkaz na zpojazdnenie a konfiguráciu loop zariadení
  - `-f` - prepínač, ktorý nájde a vypíše voľné loop zariadenie (ak žiadne nenájde, tak vytvorí nové)

Pripojenie súboru k loop zariadeniu (stale sa nachádzam v priečinku `~/cviko2`):

```
sudo losetup /dev/loop0 fs.crypt
```

- `/dev/loop0` - názov loop zariadenia
- `fs.crypt` - názov súboru, ktorý sa pripojí

Zobrazenie blokových zariadení pomocou príkazu `lsblk -a`:

```
[rocky@rocky-student-6 cviko2]$ lsblk -a
NAME        MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
loop0         7:0    0   32M  0 loop
└─crypt_fs  253:0    0   16M  0 crypt
loop1         7:1    0    0B  0 loop
vda         252:0    0   10G  0 disk
├─vda1      252:1    0  100M  0 part  /boot/efi
├─vda2      252:2    0 1000M  0 part  /boot
├─vda3      252:3    0    4M  0 part
├─vda4      252:4    0    1M  0 part
└─vda5      252:5    0  8.9G  0 part  /
[rocky@rocky-student-6 cviko2]$
```

Vytvorenie šifrovaného (LUKS) súborového systému v subore na `/dev/loop0`:

```
sudo cryptsetup luksFormat /dev/loop0 --label "crypt_fs"
```

- `cryptsetup` - príkaz na správu šifrovaných zariadení pomocou LUKS/dm-crypt
  - `luksFormat` - prepínač na naformátovanie zariadenia na LUKS
  - `/dev/loop0` - názov zariadenia, ktoré sa šifruje
  - `--label` - prepínač, ktorý určuje label zariadenia
  - `"crypt_fs"` - label zariadenia

```
sudo cryptsetup open /dev/loop0 crypt_fs
```

- `open` - prepínač na "otvorenie" šifrovaného zariadenia (namapuje ho na `/dev/mapper/crypt_fs`)

Vytvorenie `ext4` súborového systému v šifrovanej časti:

```
sudo mkfs.ext4 -L crypt_fs -m 3 /dev/mapper/crypt_fs
sudo tune2fs -c 15 /dev/mapper/crypt_fs
```

- `mkfs.ext4` - príkaz na vytvorenie súborového systému (v tomto pripade ext4)
  - `-L` - prepínač, ktorý určuje label súborového systému
  - `crypt_fs` - label súborového systému
  - `-m` - prepínač, ktorý určuje percentuálnu rezerváciu kapacity pre super-usera

    - `3` - predstavuje 3% rezerváciu
    - `/dev/mapper/crypt_fs` - názov zariadenia, ktoré sa formátuje
- `tune2fs` - príkaz na nastavenie parametrov súborového systému
    - `-c` - prepínač, ktorý určuje počet pripojení pred testom súborového systému
    - `15` - počet pripojení

Zobrazenie stavu šifrovaného súborového systému pomocou príkazu `cryptsetup status crypt_fs`:

```
[rocky@rocky-student-6 cviko2]$ sudo cryptsetup status crypt_fs
/dev/mapper/crypt_fs is active.
  type:    LUKS2
  cipher:  aes-xts-plain64
  keysize: 512 bits
  key location: keyring
  device:  /dev/loop0
  loop:    /home/rocky/cviko2/fs.crypt
  sector size:  512
  offset:  32768 sectors
  size:    32768 sectors
  mode:    read/write
[rocky@rocky-student-6 cviko2]$
```

Nasledujúci príkaz vytvorí priečinok `/tmp/crypt` a pripojí do neho šifrovaný súborový systém s povolením ACL, uzívateľských kvót a bez možnosti spustenia súborov:

```
sudo mkdir -p /tmp/crypt
sudo mount -o acl,usrquota,noexec /dev/mapper/crypt_fs /tmp/crypt
```

- `mount` - príkaz na pripojenie súborového systému
    - `-o` - prepínač, ktorý určuje možnosti pripojenia (options)
    - `acl` - povolenie ACL
    - `usrquota` - povolenie uzívateľských kvót
    - `noexec` - zakáže spustenie súborov
    - `/dev/mapper/crypt_fs` - názov zariadenia, ktoré sa pripája
    - `/tmp/crypt` - cesta, kam sa pripája

Zobrazenie pripojených súborových systémov pomocou príkazu `lsblk -a` (pripojený do `/tmp/crypt`):

```
[rocky@rocky-student-6 crypt]$ lsblk -a
NAME        MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
loop0         7:0    0   32M  0 loop
└─crypt_fs  253:0    0   16M  0 crypt /tmp/crypt
loop1         7:1    0    0B  0 loop
vda         252:0    0   10G  0 disk
├─vda1      252:1    0  100M  0 part  /boot/efi
├─vda2      252:2    0 1000M  0 part  /boot
├─vda3      252:3    0    4M  0 part
├─vda4      252:4    0    1M  0 part
└─vda5      252:5    0  8.9G  0 part  /
[rocky@rocky-student-6 crypt]$
```

Na otestovanie spustitelnosti súborov treba pomocou editora vytvorit subor v `/tmp/crypt` a do neho vložiť nasledujúci kód:

```
#!/bin/bash

echo "test in /tmp/crypt"
```

Musíme nastaviť prístupové práva, aby bol súbor spustiteľný a následne ho spustiť:

```
chmod +x /tmp/crypt/test.sh
/tmp/crypt/test.sh
```

- `chmod` - príkaz na zmenu prístupových práv
  - `+x` - pridá právo na spustenie pre všetkých

Otestovanie spustitelnosti súboru v `/tmp/crypt` (nefunguje ani pomocou `sudo`):

```
[rocky@rocky-student-6 crypt]$ lss
total 18K
drwxr-xr-x.  3 root root 1.0K Sep 24 14:01 .
drwxrwxrwt. 11 root root 4.0K Sep 24 13:55 ..
drwx------.  2 root root  12K Sep 23 23:22 lost+found
-rwxr-xr-x.  1 root root   39 Sep 24 14:01 test_run.sh
[rocky@rocky-student-6 crypt]$ cat test_run.sh
#!/bin/bash

echo "test in /tmp/crypt"
[rocky@rocky-student-6 crypt]$ ./test_run.sh
-bash: ./test_run.sh: Permission denied
[rocky@rocky-student-6 crypt]$ sudo !!
sudo ./test_run.sh
sudo: unable to execute ./test_run.sh: Permission denied
[rocky@rocky-student-6 crypt]$
```

Zadanie č.2

- **Úlohy:**
  - Vytvorte adresáre */tmp/crypt/prbit* a */tmp/crypt/prbit/public* a zabezpečte, aby:
    - vlastník bol root a mal všetky oprávnenia
    - členovia skupiny *studenti* nevideli obsah adresára */tmp/crypt/prbit* (ani ho nemohli meniť), ale mali práva na čítanie adresára */tmp/crypt/prbit/public*
    - ostatní nemali žiaden prístup
  - Vytvorte súbor */var/log/test.log* a zabezpečte, aby:
    - vlastník a vlastniaca skupina bola *root a* ostatní nemali žiadne práva
    - *admin*, ktorý nie je členom skupiny *root* mohol čítať obsah súboru
    - do súboru bolo možné obsah len dopĺňať (nie mazať ani meniť)
  - Použite atribúty a zoznamy riadenia prístupu.

Vytvorenie adresára `/tmp/crypt/prbit` a `/tmp/crypt/prbit/public` s prístupovými právami (vlastník je `root` pretože som použil `sudo`):

```
sudo mkdir /tmp/crypt/prbit
sudo mkdir /tmp/crypt/prbit/public
sudo chmod 700 /tmp/crypt/prbit
sudo chmod 750 /tmp/crypt/prbit/public
```

- `chmod` - príkaz na zmenu prístupových práv
  - `700` - nastavenie prístupových práv na úplny prístup pre vlastníka a ostatným zakáže prístup

- `750` - nastavenie prístupových práv na úplny prístup pre vlastníka, čítanie a spustenie pre skupinu a ostatným zakáže prístup

Overenie prístupových práv, že vlastník je `root`:

```
[rocky@rocky-student-6 ~]$ sudo ls -alh1 --group-directories-first /tmp/crypt -R
/tmp/crypt:
total 19K
drwxr-xr-x.  4 root root 1.0K Sep 24 14:13 .
drwxrwxrwt. 11 root root 4.0K Sep 24 13:55 ..
drwx------.  2 root root  12K Sep 23 23:22 lost+found
drwx------.  3 root root 1.0K Sep 24 14:13 prbit
-rwxr-xr-x.  1 root root   39 Sep 24 14:01 test_run.sh

/tmp/crypt/lost+found:
total 13K
drwx------. 2 root root  12K Sep 23 23:22 .
drwxr-xr-x. 4 root root 1.0K Sep 24 14:13 ..

/tmp/crypt/prbit:
total 3.0K
drwx------. 3 root root 1.0K Sep 24 14:13 .
drwxr-xr-x. 4 root root 1.0K Sep 24 14:13 ..
drwx------. 2 root root 1.0K Sep 24 14:13 public

/tmp/crypt/prbit/public:
total 2.0K
drwx------. 2 root root 1.0K Sep 24 14:13 .
drwx------. 3 root root 1.0K Sep 24 14:13 ..
[rocky@rocky-student-6 ~]$
```

Nastavenie prístupových práv pre skupinu `studenti` a nastavenie prístupových práv pre ostatných:

```
sudo setfacl -m g:studenti:rx /tmp/crypt/prbit/public
sudo setfacl -m g::rx /tmp/crypt/prbit/public
sudo chown :studenti /tmp/crypt/prbit/public
```

- `setfacl` - príkaz na nastavenie prístupových práv (set file access control list)
  - `-m` - prepínač, ktorý určuje, že sa nastavujú nové prístupové práva
  - `g:studenti:rx` - nastavenie prístupových práv pre skupinu `studenti` na čítanie a spustenie (g - group)
  - `g::rx` - nastavenie prístupových práv pre všetky skupiny na čítanie a spustenie
- `chown` - príkaz na zmenu vlastníka a skupiny súboru
  - `:studenti` - nastavenie skupiny na `studenti` súboru `/tmp/crypt/prbit/public`

Overenie prístupových práv:

```
[rocky@rocky-student-6 crypt]$ sudo ls -alh1 --group-directories-first /tmp/crypt/prbit -R
/tmp/crypt/prbit:
total 4.0K
drwx------. 3 root root     1.0K Sep 24 14:13 .
drwxr-xr-x. 4 root root     1.0K Sep 24 14:13 ..
drwxr-x---+ 2 root studenti 1.0K Sep 24 14:13 public

/tmp/crypt/prbit/public:
total 3.0K
drwxr-x---+ 2 root studenti 1.0K Sep 24 14:13 .
drwx------. 3 root root     1.0K Sep 24 14:13 ..
[rocky@rocky-student-6 crypt]$ sudo getfacl /tmp/crypt/prbit -R
getfacl: Removing leading '/' from absolute path names
# file: tmp/crypt/prbit
# owner: root
# group: root
user::rwx
group::---
other::---

# file: tmp/crypt/prbit/public
# owner: root
# group: studenti
user::rwx
group::r-x
group:studenti:r-x
mask::r-x
other::---

[rocky@rocky-student-6 crypt]$
```

Vytvorenie súboru `/tmp/crypt/prbit/public/test.txt` pomocou `touch` a nastavenie prístupových práv (vlastník je `root` pretože som použil `sudo`):

```
sudo touch /var/log/test.log
sudo chmod 600 /var/log/test.log
sudo setfacl -m u:admin:r /var/log/test.log
sudo chattr +a /var/log/test.log
```

- `chmod 600` - nastavenie prístupových práv na čítanie a zápis iba pre vlastníka
- `setfacl` - príkaz na nastavenie prístupových práv (set file access control list)
  - `u:admin:r` - nastavenie prístupových práv pre používateľa `admin` na čítanie
- `chattr` - príkaz na zmenu atribútov súboru
  - `+a` - pridanie atribútu `append-only` na súbor

Overenie prístupových práv:

```
[rocky@rocky-student-6 log]$ lss /var/log/test.log
-rw-r-----+ 1 root root 0 Sep 24 15:00 /var/log/test.log
[rocky@rocky-student-6 log]$ getfacl /var/log/test.log
getfacl: Removing leading '/' from absolute path names
# file: var/log/test.log
# owner: root
# group: root
user::rw-
user:admin:r--
group::---
mask::r--
other::---

[rocky@rocky-student-6 log]$
```